National Infrastructure Protection Center
CyberNotes

Issue #2002-25 *December 16, 2002*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between November 22 and between December 13, 2002. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
3Com[1]	Multiple	3Com SuperStack 3 NBX 4.0.17, 4.1.4	A Denial of Service vulnerability exists in the FTPD server when a malicious user sends a CEL parameter of excessive length. It may also be possible to execute arbitrary code.	No workaround or patch available at time of publishing.	3Com SuperStack 3 Denial of Service	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[1] Bugtraq, December 2, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
3D3.COM Pty Ltd.[2]	Windows	Shop Factory 5.5, 5.6	A vulnerability exists because the contents of shopping carts can be modified by customers, which could let a remote malicious user modify the price of items.	No workaround or patch available at time of publishing.	ShopFactory Shopping Cart Cookie Price Manipulation	Medium	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
akfingerd[3]	Unix	akfingerd 0.5	Multiple vulnerabilities exist: a remote Denial of Service vulnerability exists when connecting to the daemon via finger; a Denial of Service vulnerability exists when the server is caused to write to a socket that is not a listening client; and a file disclosure vulnerability exists due to the supplementary group privileges not being dropped and insufficient sanity checks of the '.plan' file, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Akfingerd Multiple Vulnerabilities	Low/ Medium (Medium if sensitive informa-tion can be obtained)	Bug discussed in newsgroups and websites. There is no exploit code required.
AlCastle.com[4]	Unix	Aldap 0.09	A vulnerability exists in the database bind() function in 'config.inc' because it is possible to bypass authentication, which could let an unauthorized remote malicious user obtain administrative privileges.	Upgrade available at: http://alcastle.com/redirect.php?url=public/aldap/0_09/aldap-0.09-2.tar.gz	Aldap Contact Manager Authentication Bypass	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Apache Software Founda-tion[5]	Unix	Apache 1.3, 1.3.11, 1.3.12, 1.3.14, 1.3.17-1.3.20. 1.3.22-1.3.27, mod_jk 1.2, Tomcat 4.0-4.0.5, 4.1, 4.1.10, 4.1.12	A Denial of Service vulnerability exists when mod_ik is used due to design problems in the module.	Apache Software Foundation Upgrade mod_jk 1.2.1 available at: http://jakarta.apache.org/builds/jakarta-tomcat-connectors/jk/release/v1.2.1/	Apache/ Tomcat Mod_JK Chunked Encoding Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.

[2] Securiteam, December 5, 2002.
[3] Bugtraq, December 5, 2002.
[4] SecurityTracker Alert ID, 1005727, November 29, 2002.
[5] Qualys Security Advisory, QSA-2002-12-04, December 4, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
APP[6]	Unix	APBoard 2.0 2	A vulnerability exists in the 'useraction.php' script due to a failure to properly check user credentials, which could let unauthorized malicious users read postings in internal forums.	No workaround or patch available at time of publishing.	APBoard Unauthorized Thread Reading	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Apple Software[7]	MacOS X 10.2	MacOS X 10.2.2, Server 10.2.2	A Denial of Service vulnerability exists when a malicious user creates a directory, descends it, creates another directory of the same name, and then attempts to move the directory up one level in the hierarchy.	No workaround or patch available at time of publishing.	Mac OS X Directory Kernel Panic Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
apt-www-proxy[8]	Unix	apt-www-proxy 0.1	Multiple vulnerabilities exist: a Denial of Service vulnerability exists when a NULL HTTP request is submitted; and a format string vulnerability exists in the awp_log() function due to an incorrect use of the syslog() function, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	apt-www-proxy NULL HTTP Request Denial of Service & Format String	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required for the Denial of Service vulnerability.
Boozt![9]	Unix	Boozt! Standard 0.9.8	A buffer overflow vulnerability exists in the 'index.cgi' script when a parameter is submitted that is of excessive length, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Boozt index.cgi Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Canna[10]	Unix	Canna 3.5 b2	A buffer overflow vulnerability exists due to a lack of validation of requests, which could let a malicious user execute arbitrary code. with 'bin' level privileges. *Note: Canna is typically installed only when Japanese language support is enabled.*	**RedHat:** ftp://updates.redhat.com/	Canna Server Local Buffer Overflow CVE Name: CAN-2002-1158, CAN-2002-1159	**High**	Bug discussed in newsgroups and websites.
Carnegie Mellon University[11]	Unix	Cyrus IMAP Server 1.4, 2.1.10	A buffer overflow vulnerability exists prior to authentication because overly long strings are not properly handled, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Cyrus IMAPD Pre-Login Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[6] Bugtraq, December 6, 2002.
[7] SecurityFocus, December 7, 2002.
[8] INetCop Security Advisory, 2002-0x82-009, December 10, 2002.
[9] SecurityFocus, November 29, 2002.
[10] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:246-18, December 4, 2002.
[11] CERT/CC Vulnerability Note, VU#740169, December 3, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cisco Systems[12]	Multiple	Cisco 7600, Catalyst 6500 , IOS 12.1 (9)E, (8)E, (13.4)E, (12)E, (11)E, (10)E	A Denial of Service vulnerability exists in Optical Service Module (OSM) Line Cards when an irregularly constructed network packet is processed.	Upgrade information available at: http://www.cisco.com/warp/public/707/osm-lc-ios-pkt-vuln-pub.shtml	Cisco OSM Line Card Header Corruption	Low	Bug discussed in newsgroups and websites.
Computer Associates [13]	Windows NT	eTrust Antivirus EE 6.0	A vulnerability exists when a specially crafted commandline argument is submitted, which could let a malicious user obtain elevated privileges and execute arbitrary programs.	Patch available at: ftp://ftp.ca.com/CAproducts/unicenter/eTrust/AntiVirus/6.0/nt/qo30577/QO30577.CAZ	eTrust Antivirus EE Privilege Escalation	**High**	Bug discussed in newsgroups and websites.
Computer Associates [14]	Unix	InoculateIT 6.0	A vulnerability exists when the system is configured with the incremental scan option, which could allow virus or Trojan code to be saved to disk, and signed as clean.	The vendor has reportedly released a patch that disables the incremental scan option. Contact the vendor for information.	InoculateIT Incremental Scan Option	Medium	Bug discussed in newsgroups and websites.
Cyrus[15]	Unix	SASL 2.1.9	Several buffer overflow vulnerabilities exist: a vulnerability exists in the SASL Library due to insufficient bounds checking while sanitizing usernames, which could let a malicious user execute arbitrary instructions; (*Note: This issue only exists if the default realm is set.)* a vulnerability exists in the SASL library due to a failure to allocate sufficient memory when it is required to escape characters, which could let a malicious user execute arbitrary code; and a vulnerability exists when log files are generated due to a failure to allocate sufficient memory, which could let a malicious user corrupt memory and possibly cause inaccurate logs to be created.	Upgrade available at: ftp://ftp.andrew.cmu.edu/pub/cyrus-mail/cyrus-sasl-2.1.10.tar.gz	Cyrus SASL Library Multiple Buffer Overflow Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Cyrusoft[16]	Unix	libSieve 2.1.2	A buffer overflow vulnerability exists in the Sieve library when a header of excessive length is submitted, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	libSieve Header Name Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[12] Cisco Security Advisory, December 11, 2002.
[13] SecurityFocus, December 4, 2002.
[14] Bugtraq, December 2, 2002.
[15] Bugtraq, December 9, 2002.
[16] Securiteam, December 5, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cyrusoft[17]	Unix	libSieve 2.1.2	Several buffer overflow vulnerabilities exist: a buffer overflow vulnerability exist in the Sieve library when an IMAP flag of excessive length is passed to the program, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability exists when excessive error messages are generated, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	libSieve Buffer Overflows	**High**	Bug discussed in newsgroups and websites.
Debian[18]	Unix	Internet Message 133.0, 141.0	A vulnerability exists due to the way Debian Internet Message (IM) creates temporary files, which could let a malicious user corrupt or modify data.	Upgrade available at: http://security.debian.org/pool/updates/main/i/im	Debian Internet Message Insecure Temporary File Creation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Deerfield [19]	Windows NT	VisNetic Website 3.5.13 .1	A vulnerability exists in the OPTIONS directory when attempting to handle a malformed request for a resource, which could let a malicious user cause a Denial of Service and possibly execute arbitrary code.	Upgrade available at: http://www.deerfield.com/download/visnetic_website/	Deerfield VisNetic Website OPTIONS Memory Corruption	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Eric Raymond [20]	Unix	bogofilter 0.9 .0.4	A vulnerability exists because temporary files are created in an insecure manner, which could let a malicious user obtain elevated privileges.	Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=62265&release_id=118794	Bogofilter Insecure Temporary File Creation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Fortres Grand Corpor-ation[21]	Windows 95/98/ME/ NT 4.0/2000, XP	Fortres 101 4.1	A vulnerability exists when the WINDOWS + F key combination is held down for an extended period of time, which could let a malicious user bypass security restrictions and obtain unauthorized access.	No workaround or patch available at time of publishing.	Fortres 101 Software Disabling Protection Circumventing	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[17] Bugtraq, December 2, 2002.
[18] Debian Security Advisory, DSA 202-2, December 6, 2002.
[19] Securiteam, December 12, 2002.
[20] bogofilter-SA-2002:01, November 29, 2002.
[21] SecurityTracker Alert ID, 1005766, December 5, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
GNU[22, 23, 24]	Unix	wget 1.5.3, 1.6, 1.7, 1.7.1, 1.8, 1.8.1, 1.8.2	A vulnerability exists due to inadequate input checks when a NLST response is received from an FTP server, which could let a remote malicious user overwrite files on the client system.	**Debian:** http://security.debian.org/pool/updates/main/w/wget **RedHat:** ftp://updates.redhat.com/ **Mandrake:** http://www.mandrakesecure.net/en/ftp.php	WGet NLST Client Side File Overwriting CVE Name: CAN-2002-1344	Medium	Bug discussed in newsgroups and websites.
gnuplot[25]	Unix	gnuplot 3.7	A buffer overflow vulnerability exists in GNUPlot that is shipped with SuSE Linux, which could let a malicious user obtain root privileges.	Upgrade available at: ftp://ftp.suse.com/pub/suse/	GNUPlot French Documentation Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Gordano[26]	Windows NT	NTMail 8.0	A vulnerability exists in 'rwords' filtering, which could let a malicious user bypass e-mail filters.	No workaround or patch available at time of publishing.	Gordano Mail Server 'rword' Filter Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
GTetrinet [27]	Unix	GTetrinet 0.4-0.4.3	Several buffer overflow vulnerabilities exist due to insufficient bounds checking, which could let a malicious user cause a Denial of Service and potentially execute arbitrary code.	Upgrade available at: http://download.sourceforge.net/gtetrinet/gtetrinet-0.4.4.tar.gz **Debian:**; http://security.debian.org/pool/updates/main/g/gtetrinet/	GTetrinet Multiple Remote Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Hewlett Packard Company [28]	Unix	HP-UX 10.10, 10.20, 11.0	A vulnerability exists in the ied program, which could let a malicious user obtain sensitive information.	Patches available at: http://itrc.hp.com PHCO_27560, PHCO_27560, PHCO_24446	HP-UX ied Information Disclosure		Bug discussed in newsgroups and websites.
Hewlett Packard Systems[29]	Unix	HP-UX 10.20, 10.24, 11.04, 11.0, 11.11	A Denial of Service vulnerability exists in the xntpd program.	Patches available at: http://itrc.hp.com PHNE_24510, PHNE_28002, PHNE_27442, PHNE_27223, PHNE_24512	HP-UX xntpd Denial of Service	Low	Bug discussed in newsgroups and websites.

[22] Debian Security Advisory, DSA-209-1, December 13, 2002.
[23] Mandrake Security Advisory, MDKSA-2002:086, December 11, 2002.
[24] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:229-10, December 10, 2002.
[25] SuSE Security Announcement, SuSE-SA:2002:047, December 6, 2002.
[26] SecurityFocus, December 11, 2002.
[27] Debian Security Advisory, DSA-205-1, December 10, 2002.
[28] Hewlett-Packard Company Security Bulletin, HPSBUX0212-227, December 3, 2002.
[29] Hewlett-Packard Company Security Bulletin, HPSBUX0212-232, December 10, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Systems[30]	Unix	HP-UX 11.0, 11.11	A vulnerability exists because the installation of HP-UX Visualize Conference may leave certain directories with insecure permissions, which could let a malicious user obtain unauthorized access and elevated privileges.	Change ownership and permissions as follows: /etc/dt 755 bin/bin /etc/dt/appconfig 755 root/sys /etc/dt/appconfig/icons 755 root/sys /etc/dt/appconfig/icons/C 755 root/sys /etc/dt/appconfig/types 755 root/sys /etc/dt/appconfig/types/C 755 root/sys	HP-UX Visualize Conference Insecure Default Permissions	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Ikonboard .com[31]	Unix	ikonboard 3.1.1	A vulnerability exists because HTML is not properly sanitized from user profile photo URIs, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Ikonboard User Profile Photo URI HTML Injection	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Ikonboard .com[32]	Unix	ikonboard 3.1.1	A vulnerability exists in the X-Forwarded-For: HTTP header proxy fields because HTML is not properly sanitized when the header field is logged, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Ikonboard X-Forwarded-For: Proxy Header Field HTML Injection	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
KDE[33] ***More vendors release patches[34, 35, 36]***	**Unix**	**KDE 2.1-2.2.2, 3.0-3.0.4**	**A vulnerability exists in the KIO subsystem rlogin and telnet protocols, which could let a remote malicious user execute arbitrary commands.**	**KDE:** **http://download.kde.org/stable/3.0.5/** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php** ***RedHat:*** ***SRPMS:*** **ftp://updates.redhat.com/** ***Debian:*** **http://security.debian.org/pool/updates/main/k/kdelibs/**	**KDE KIO Subsystem Network Protocol Implementation**	**High**	**Bug discussed in newsgroups and websites. There is no exploit code required.**
KisMAC [37]	Unix	KisMAC 0.02a, 0.01c, 0.01b, 0.01a	A vulnerability exists when the Apple Package Manager is used to install the application because file permissions are changed to unsafe modes, which could let a malicious user obtain sensitive information.	Upgrade available at: http://www.binaervarianz.de/projekte/programmieren/kismac	KisMAC Insecure File Permissions	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[30] Hewlett-Packard Company Security Bulletin, HPSBUX0212-231, December 11, 2002.
[31] SecurityFocus, December 9, 2002.
[32] SecurityFocus, December 9, 2002.
[33] KDE Security Advisory, November 11, 2002
[34] Mandrake Linux Security Update Advisory, MDKSA-2002:079, November 21, 2002
[35] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:220-40, December 4, 2002.
[36] Debian Security Advisory, DSA 204-1, December 5, 2002.
[37] SecurityTracker Alert ID, 1005764, December 5, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Kunani[38]	Windows	Kunani FTP Server 1.0.10	A Directory Traversal vulnerability exists, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Kunani FTP Server Directory Traversal	Medium	Bug discussed in newsgroups and websites. Vulnerability may be exploited via a FTP client.
Larry Wall[39]	Unix	Perl 5.6	An information disclosure vulnerability exists in SuidPerl, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	SuidPerl Information Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Lawson Software [40]	Unix	Lawson Financials 8.0	A vulnerability exists in some default configurations because data held in third-party relational databases is stored insecurely, which could let an unauthorized malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Lawson Financials Account Credentials World Accessible	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Linksys[41]	Multiple	BEFN2PS4 1.42.7, BEFSX41 1.43, 1.43.3, 1.43.4, BEFW114 1.4.2 .7, 1.4.3, 1.43.3, Etherfast BEFSR11 Router 1.42.7, 1.43, 1.43.3, EtherFast BEFSR41 Router 1.42.7, 1.43, 1.43.3, EtherFast BEFSR81 Router, EtherFast BEFSR81 Router 2.42.7, BEFSRU31 Router 1.42.7, 1.43, 1.43.3	Several vulnerabilities exist: a buffer overflow vulnerability exists due to insufficient allocation of memory, which could let a malicious user execute arbitrary code; a vulnerability exists because no authentication is required to access a xml page, which could let a remote malicious user obtain unauthorized access; a buffer overflow vulnerability exists due to insufficient allocation of space for local buffers, which could let a malicious user change configuration information on the vulnerable device; and a Denial of Service vulnerability exists due to insufficient bounds checking when copying user-supplied input to memory.	Upgrade available at: http://www.linksys.com/download/	Multiple Linksys Vulnerabilities	Medium **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

[38] Bugtraq, December 10, 2002.
[39] SecurityFocus, November 29, 2002.
[40] Bugtraq, December 2, 2002.
[41] CORE Security Technologies, CORE-20021005, December 3, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Macro-media[42]	Multiple	ColdFusion Server MX 6.0, JRun 4.0, 4.0SP1a, 4.0 SP1	A Denial of Service vulnerability exists in the XML parser that is used by these products.	Upgrade available at: http://download.macromedia.com/pub/security/jrun/40/MPSB02-14_JRun.zip	JRun 4/ ColdFusion XML Parser Denial of Service	Low	Bug discussed in newsgroups and websites.
Microsoft [43]	Windows 95/98/ME/ NT 4.0/2000, XP	2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Profes-sional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3, Windows 95, 95 SR2, 98, 98SE, ME, NT Enterprise Server 4.0 SP1-SP6a, NT Server 4.0 SP1-SP6a, NT Terminal Server 4.0 SP1-SP6a, NT Work-station 4.0 SP1-SP6a, XP Home SP1, XP Professiona l SP1	Multiple vulnerabilities exist: a vulnerability exists because it's possible for an untrusted Java applet to access COM objects, which could let a malicious user obtain control over the machine; two vulnerabilities exists because it is possible to spoof the location specified in CODEBASE parameter in the APPLET tag, which could let a malicious user obtain sensitive information; a vulnerability exists due to a flaw in the Virtual Machine's URL parser, which could let a malicious user intercept any traffic that the user would send to the trusted site; a vulnerability exists because Java Database Connectivity APIs don't properly regulate who can call them, which could let a malicious user obtain sensitive information; a Denial of Service vulnerability exists due to insufficient security checks in the VM; a vulnerability exists because VM doesn't prevent untrusted applets from accessing the user.dir system property, which could let a malicious user sensitive information; and a vulnerability exists because it is possible for a Java applet to create an incorrectly initialized Java object, which could let a malicious user cause Internet Explorer to fail.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-069.asp	Java Virtual Machine Multiple Vulnerabilities CVE Names: CAN-2002-1254, CAN-2002-1257, CAN-2002-1258, CAN-2002-1259, CAN-2002-1260, CAN-2002-1261, CAN-2002-1263	Low/ Medium/ **High** (Medium if sensitive informa-tion can be obtained and **High if control can be obtained over the system)**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Microsoft [44]	Windows XP	Windows XP Home, XP Home SP1, XP Profes-sional, XP Profes-sional SP1	An information disclosure vulnerability exists in the wireless LAN feature, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Microsoft Windows XP Wireless LAN Information Disclosure	Medium	Bug discussed in newsgroups and websites.

[42] Macromedia Advisory, MPSB02-14, December 11, 2002.
[43] Microsoft Security Bulletin, MS02-069, December 11, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [45]	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.5, 6.0	A vulnerability exists because it is possible to bypass Internet Explorer's cross-domain security model when using object caching in scripting flaw due to incomplete security checks, which could let a malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the workaround can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-068.asp	Internet Explorer Object Caching CVE Name: CAN-2002-1262	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Microsoft [46]	Windows 98/ME/NT 4.0/2000	Internet Explorer 6.0, 6.0 SP1	A vulnerability exists in the showModalDialog and ShowModelessDdialog functions when script code is injected into the style parameters due to improper checks, which could let a remote malicious user execute arbitrary JavaScript and HTML code	No workaround or patch available at time of publishing.	Microsoft Internet Explorer Dialog Style Same Origin Policy Bypass	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft [47]	Windows 98/ME/NT 4.0/2000, XP	Outlook 2002, 2002 SP1&SP2	A Denial of Service vulnerability exists if an e-mail message is submitted that contains a partially malformed header.	Frequently asked questions regarding this vulnerability and the workaround can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-067.asp	Outlook 2002 E-mail Header Processing Denial of Service CVE Name: CAN-2002-1255	Low	Bug discussed in newsgroups and websites.
Microsoft [48]	Windows NT 4.0/2000, XP	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Profes-sional, SP1-SP3, 2000 Server, SP1-SP3, XP Home, XP Home SP1, XP Profes-sional, XP Profes-sional SP1	A vulnerability exists because it's possible for one process in the interactive desktop to use a WM_TIMER message to cause another process to execute a callback function at the address of its choice, even if the second process did not set a timer, which could let a malicious user obtain full administrative privileges.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-071.asp	Windows 2000/XP WM_TIMER Message Handling CVE Name: CAN-2002-1230	**High**	**Bug discussed in newsgroups and websites. Proofs of Concept exploit scripts have been published.**

[44] SNS Advisory No.60, December 5, 2002.
[45] Microsoft Security Bulletin, MS02-068 V2.0, December 6, 2002.
[46] Bugtraq, December 3, 2002.
[47] Microsoft Security Bulletin, MS02-067, December 4, 2002.
[48] Microsoft Security Bulletin, MS02-071, December 11, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [49] *Microsoft releases bulletin* [50]	**Windows NT 4.0/2000, XP**	**Windows 2000 Advanced Server, SP1&2, Datacenter Server, SP1&2, Profes-sional, SP1&2, 2000 Server, SP1&2, 2000 Server Japanese Edition, 2000 Terminal Services, SP1&2, NT Enterprise Server 4.0, SP1-SP6a, NT Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, NT Work-station 4.0, SP1-SP6a, Windows XP, 64-bit Edition, Home, Profes-sional**	**A design error exists in the Win32 API inter-window message passing system, which could let a malicious user obtain elevated privileges.**	***Frequently asked questions regarding this vulnerability and the patch can be found at:*** **http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-071.asp**	**Microsoft Windows Message Subsystem Design Error**	**Medium**	**Bug discussed in newsgroups and websites. Exploit script has been published.** **Vulnerability has appeared in the press and other public media.**
Microsoft [51]	Windows XP	Windows XP Home, XP Home SP1, Profes-sional, Profes-sional SP1	A vulnerability exists in the Fast User Switching (FUS) option that allows users that have been downgraded from the Administrator to a normal users to still use the Task Manager, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Windows XP Fast User Switching Process Viewing	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[49] Bugtraq, August 6, 2002.
[50] Microsoft Security Bulletin, MS02-071, December 11, 2002.
[51] Securiteam, December 1, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [52]	Windows 2000, XP	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Profes-sional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3, XP 64-bit Edition, XP Home, XP Profes-sional	A vulnerability exists in the negotiation process because it is possible to cause the signing of Server Message Block (SMB) packets to be disabled, even when it is required by the host, which could let a malicious user obtain sensitive information.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-070.asp	Windows SMB Signing CVE Name: CAN-2002-1256	Medium	Bug discussed in newsgroups and websites.
Mobydisk [53]	Windows	Moby Netsuite 1.0, 1.2	A buffer overflow vulnerability exists when malformed POST requests are submitted, which could let a remote malicious user cause a Denial of Service.	No workaround or patch available at time of publishing.	Moby NetSuite POST Handler Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Mollen-soft Software[54]	Windows NT	Enceladus Server Suite 2.6.1	A Directory Traversal vulnerability exists due to improper sanitization of web requests, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Enceladus Server Suite Directory Traversal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Mollen-soft Software[55]	Windows	Enceladus Server Suite 3.9	A buffer overflow vulnerability exists when an overly long value is submitted for the FTP change directory (CD) command, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Mollensoft Software Enceladus Server Suite CD Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[52] Microsoft Security Bulletin, MS02-070, December 11, 2002.
[53] Securiteam, December 1, 2002.
[54] Securiteam, December 11, 2002.
[55] Bugtraq, December 9, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[56]	Unix	OpenBSD OpenBSD 3.0; Sun Solaris 2.6, 2.6_x86, 7.0, 7.0_x86	A vulnerability exists because several FTP clients distributed with various operating systems may handle NLST FTP responses in an insecure manner, which could let a malicious server overwrite key files to cause a Denial of Service or, in some cases, gain privileges by modifying executable files.	No workaround or patch available at time of publishing.	Multiple Vendor FTP Client Side File Overwriting CVE Name: CAN-2002-1345	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors[57] ***More advisories released[58, 59, 60]***	**Unix**	**Solaris 2.5.1, 2.5.1_x86, _ppc, 2.6, 2.6 _x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86 Update 2; XFree86 X11R6 3.3, 3.3.2-3.3.5; *HP-UX 10.10, 10.20, 10.24, 11.04, 11.0, 11.11, 11.22; SGI IRIX 6.5, 6.5.1-6 .5.13***	**A buffer overflow vulnerability exists in the XFS font server, fs.auto used by multiple vendors, which could let a remote malicious user execute arbitrary commands.**	**XFree:** ftp://ftp.xfree86.org/pub/XFree86/4.2.0/Xinstall.sh **Note: This is just the installation script. You must acquire the platform specific binary for this distribution from:** ftp://ftp.xfree86.org/pub/XFree86/4.2.0/binaries/ **or** http://ftp.xfree86.org/pub/XFree86/4.2.0/binaries **To determine which distribution you need to download, obtain the installation script (Xinstall.sh) and run the command: sh Xinstall.sh -check** ***Hewlett Packard (temporary patch):*** ftp://xfs:xfs1@hprc.external.hp.com/ ***SGI:*** ftp://patches.sgi.com/support/free/security/advisories/20021202-01-I	**Multiple Vendor fs.auto Remote Buffer Overrun** CVE Name: CAN-2002-1317	**High**	**Bug discussed in newsgroups and websites.**

[56] SGI Security Advisory, 20021205-01-A, December 13, 2002.
[57] ISS X-Force Security Brief, November 25, 2002.
[58] SGI Security Advisory, 20021202-01-I, December 4, 2002.
[59] Hewlett-Packard Company Security Bulletin, HPSBUX0212-228, December 6, 2002.
[60] Sun(sm) Alert Notification, 48879, November 25, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[61] [62] *More patches released*[63], [64], [65], [66], [67] *Proof of Concept exploit has been published.*[68] *HP releases bulletin*[69] *More patches released*[70], [71], [72], [73], [74] *SCO releases patch*[75]	Windows NT 4.0/2000, Unix	Apache Software Foundation Apache 1.3.20, 1.3.22-1.3.26; Oracle Internet Application Server 1.0.2.1, 1.0.2.0, 8i Enterprise Edition 8.1.7.1.0, 8.1.7.0.0, 9i Application Server, 1.0.2.2, 1.0.2.1s, 1.0.2, 9.0.2, 9.0.2 release 2, 9iAS Reports 9.0.2 .1, Oracle8 8.1.7, 8.1.7.1, 8.1.7, Oracle9i Release 2 9.2 .2, 9.0.2	Multiple vulnerabilities exist: a Denial of Service vulnerability exists due to the way the Apache scorecard is handled; a Cross-Site Scripting vulnerability exists due to improper sanitization of SSI error pages, which could let a malicious user execute arbitrary HTML or JavaScript code; and a buffer overflow vulnerability exists in the ab.c web benchmarking support utility, which could let a malicious user execute arbitrary code.	**Apache Software Foundation:** http://www.apache.org/dist/httpd/apache_1.3.27.tar.gz **Oracle Corporation:** Oracle has stated that fixes for affected software will be available October 8, 2002 through metalink. ***OpenPKG:*** ftp://ftp.openpkg.org/release/1.0/UPD/ ***Engarde Secure Linux:*** ftp://ftp.engardelinux.org/pub/engarde/stable/updates/i386/apache-1.3.27-1.0.32.i386.rpm ***Mandrake:*** http://www.mandrakesecure.net/en/ftp.php *FreeBSD:* ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/i386/packages-4-stable/All/ *Oracle:* http://metalink.oracle.com ***Trustix:*** http://www.trustix.net/pub/Trustix/updates/ *Hewlett Packard:* http://www.software.hp.com/ISS_products_list.html *Debian:* http://security.debian.org/pool/updates/main/a/apache/a http://security.debian.org/pool/updates/main/a/apache-ssl *SGI:* ftp://patches.sgi.com/support/free/security/advisories/20021105-01-I ***SCO:*** ftp://ftp.sco.com/pub/updates/OpenLinux/3.1.1/Workstation/CSSA-2002-056.0/	Apache Web Server Multiple Vulnerabilities CVE Names: CAN-2002-0839, CAN-2002-0840, CAN-2002-0843	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. *Proof of Concept exploit has been published for the Cross-Site Scripting Vulnerability.*

[61] iDEFENSE Security Advisor, 10.03.2002, October 3, 2002.
[62] OpenPKG Security Advisory, OpenPKG-SA-2002.009, October 4, 2002.
[63] EnGarde Secure Linux Security Advisory, ESA-20021007-024, October 7, 2002.
[64] FreeBSD Security Notice, FreeBSD-SN-02:06, October 10, 2002.
[65] Mandrake Linux Security Update Advisory, MDKSA-2002:068, October 16, 2002.
[66] Oracle Security Alert #45, October 4, 2002.
[67] Trustix Secure Linux Security Advisory, 2002-0069, October 17, 2002.
[68] SecurityFocus, October 30, 2002.
[69] Hewlett-Packard Company Security Bulletin, HPSBUX0210-224, October 30, 2002.
[70] Debian Security Advisory, DSA 187-1, November 4, 2002.
[71] Debian Security Advisory, DSA 188-1, November 5, 2002.
[72] SGI Security Advisory, 20021105-01-I, November 12, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [76, 77] ***More vendors release upgrades*** [78]	**Unix**	**Hewlett Packard Secure OS software for Linux 1.0; RedHat Linux 6.2, 6.2 sparc, i386, alpha,7.0, 7.0 i386, alpha, 7.1, 7.1 ia64, i386, alpha, 7.2, 7.2 ia64, i386, 7.3, 7.3 i386, 8.0, 8.0 i386**	**A vulnerability exists in 'dvips' when a maliciously constructed file is passed to the lpd daemon, which could let a malicious user execute arbitrary commands.**	**Updates available at: ftp://updates.redhat.com/** ***Debian:*** http://security.debian.org/pool/updates/main/t/	**dvips Arbitrary Command Execution** **CVE Name: CAN-2002-0836**	**High**	**Bug discussed in newsgroups and websites.**
Mustata Bogdan,[79]	Multiple	Zeroo HTTP Server 1.5	A Directory Traversal vulnerability exists due to a failure to properly sanitize web requests, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Zeroo HTTP Server Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit scripts have been published.
myServer [80]	Windows NT	myServer 0.2, 0.11	A Directory Traversal vulnerability exists due to a failure to properly sanitize web requests, which could let al malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	myServer Directory Traversal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Netfilter. org[81]	Unix	Linux kernel 2.4, 2.4.1-2.4.19, 2.5.0-2.5.31	A vulnerability exists in the IP Queuing module due to insufficient checking of the integrity of the privileged process, which could let a malicious user obtain sensitive information.	Upgrades available at: http://www.kernel.org/pub/linux/kernel/v2.4/linux-2.4.20.tar.gz and http://www.kernel.org/pub/linux/kernel/v2.5/linux-2.5.32.tar.gz	Linux Netfilter/ IPTables IP Queuing Arbitrary Network Traffic Reading	Medium	Bug discussed in newsgroups and websites.
Network Associ-ates,[82]	Windows 95/98/ME/ NT 4.0/2000, XP	McAfee VirusScan 4.5.1	A vulnerability exists in WebScanX, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	VirusScan WebScanX Code Execution	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[73] Debian Security Advisory, DSA 195-1, November 13, 2002.
[74] Gentoo Linux Security Announcement, 200211-003, November 12, 2002.
[75] SCO Security Advisory, CSSA-2002-056.0, December 5, 2002.
[76] Hewlett Packard Systems Security Bulletin, HPSBTL0210-073, October 15, 2002.
[77] RedHat Security Advisory, RHSA-2002:194-18, October 10, 2002.
[78] Debian Security Advisory DSA 207-1, December 11, 2002.
[79] Securiteam, December 4, 2002.
[80] INetCop Security Advisory #2002-0x82-010, December 11, 2002.
[81] Netfilter Core Team Security Advisory, December 3, 2002.
[82] Bugtraq, November 29, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Open LDAP[83]	Unix	OpenLDAP 2.0- 2.0.23	Several buffer overflow vulnerabilities exist which could let a malicious user execute arbitrary code.	**SuSE:** ftp://ftp.suse.com/pub/suse/	OpenLDAP Multiple Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Pedestal Software[84]	Windows NT 4.0/2000	Integrity Protection Driver 1.2	A vulnerability exists because the Protection Driver does not start until the system has been up for 20 minutes, which could let a malicious user obtain privileged access to the system.	Upgrade available at: http://pedestalsoftware.com/download/ipd.zip	Integrity Protection Driver Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
phpBB Group[85]	Unix	phpBB 2.0.3	A Cross-Site Scripting vulnerability exists due to insufficient sanitization of user-supplied input, which could let a malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	phpBB Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
ProFTPD Project[86]	Unix	ProFTPD 1.2.1-1.2.6, 1.2.7rc3, 1.2.7 rc2, 1.2.7 rc1	A Denial of Service vulnerability exists when a specially crafted STAT command is submitted.	No workaround or patch available at time of publishing.	ProFTPD STAT Command Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Pserv[87]	Unix	Pserv 2.0 beta1, beta2, beta3, beta5	Multiple buffer overflow vulnerabilities exist due to the way data streams are handled from remote connections, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	No workaround or patch available at time of publishing.	Pserv Buffer Overflows	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Real Networks, Inc.[88]	Windows 95/98/ME/ NT 4.0/2000, XP	RealOne Player, 2.0, Player Gold for Windows 6.0.10 .505	Multiple buffer overflow vulnerabilities exist , which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Multiple Unspecified RealOne Player Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

[83] SuSE Security Announcement, SuSE-SA:2002:047, December 6, 2002.
[84] NTBugtraq, December 2, 2002.
[85] Bugtraq, December 3, 2002.
[86] Bugtraq, December 8, 2002.
[87] Securiteam, December 1, 2002.
[88] SecurityFocus, December 11, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts

SAP[89]	Unix	SAP DB 7.3 .00	A vulnerability exists in lserver due to insufficient sanity checks, which could let a malicious user execute arbitrary commands with root privileges.	The vendor has stated the following:
				Perform the following steps for each <dependent_path>
				
				$ cd <dependent_path>/pgm
				$ cp lserversrv lserver
				$ chown root lserver
				$ chmod +s lserver
					SAP DB Insufficient Checks	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

Sapio Design Ltd.[90]	Windows 95/98/NT 4.0	WebReflex 1.53	A Directory Traversal vulnerability exists due to a failure to properly sanitize web requests, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	WebReflex Directory Traversal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
SMB2 WWW[91]	Unix	SMB2 WWW 980804, 980802, 980727, 980427	A vulnerability exists in the SMB2WWW web-based Windows networking client, which could let a remote malicious user execute arbitrary commands.	Upgrade available at: http://security.debian.org/pool/updates/main/s/smb2www/	SMB2WWW Remote Command Execution	**High**	Bug discussed in newsgroups and websites.
Squirrel Mail[92]	Unix	Squirrel Mail 1.2.9	A Cross-Site Scripting vulnerability exists in the 'read_body.php' script due to a failure to properly sanitize user-supplied parameters, which could let a malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	SquirrelMail Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Sun Micro-systems, Inc.[93]	Multiple	Cobalt RaQ 4.0	A vulnerability exists in a cgi script due to improper filtering of user-supplied input, which could let a remote malicious user execute arbitrary commands. *Note: This vulnerability only affects RaQ4 servers with the RaQ4 Security Hardening Package (SHP) installed.*	Upgrade available at: http://ftp.cobalt.sun.com/pub/packages/raq4/eng/RaQ4-en-Security-2.0.1-SHP_REM.pkg	Cobalt RaQ4 Administrative Interface Command Execution	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Sun Micro-systems, Inc.[94]	Unix	Solaris 2.5.1, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	A Denial of Service vulnerability exists in applications that are linked using the libthread library.	Patches available at: http://sunsolve.sun.com/pub-cgi/	Solaris Libthread Library Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

[89] SAP DB Security Alert, December 2, 2002.
[90] Securiteam, December 8, 2002.
[91] Debian Security Advisory, DSA 203-1, December 4, 2002.
[92] Bugtraq, December 3, 2002.
[93] CERT/CC VU#810921 Note, December 11, 2002.
[94] Sun(sm) Alert Notification, 46867, December 4, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Micro-systems, Inc.[95]	Unix	Solaris 2.5.1, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0	A Denial of Service vulnerability exists due to a NULL pointer dereference.	Patches available at: http://sunsolve.sun.com/pub-cgi/	Solaris Denial of Service	Low	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[96]	Unix	Solaris 26, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	A Denial of Service vulnerability exists because some attachments are not properly handled by the mailtool.	Patches available at: http://sunsolve.sun.com	Solaris MailTool Attachment Denial of Service	Low	Bug discussed in newsgroups and websites.
Sun/ Netscape[97] ***Sun releases upgrade***[98]	**Windows, Unix**	**Netscape Communi-cator 4.0-4.8; Sun Java 2 Runtime Environ-ment 1.1-1.4**	**A vulnerability exists due to a flaw in the Bytecode Verifier, which could let a remote malicious user obtain unauthorized access and possibly execute arbitrary code.**	***Upgrade available at:*** **http://java.sun.com/j2se/1.2/**	**Sun/Netscape Java Virtual Machine Bytecode Verifier**	**Medium/ High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites.**

[95] Sun(sm) Alert Notification, 48267, December 2, 2002.
[96] Sun(sm) Alert Notification, 48216, November 27, 2002.
[97] SecurityTracker Alert IDs, 1005701 & 1005702, November 26, 2002.
[98] Sun(sm) Alert Notification, 49304, December 9, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SuSE[99] ***Debian issues advisory***[100] ***Exploit script has been published***[101] ***Debian updates advisory***[102]	**Unix**	**Linux 7.0-7.3, 8.0, 8.1**	**Two vulnerabilities exist: a vulnerability exists in the 'runlpr' utility when malicious strings are passed via the commandline which could allow a malicious user to execute arbitrary commands; and a vulnerability exists in the html2ps filter that is included in the lprng print system, which could let a remote malicious user execute arbitrary commands.** *The security update from DSA 192-1 contained a syntax error that is now fixed.*	**Patches available at: ftp://ftp.suse.com/pub/suse/** ***Debian:*** **http://security.debian.org/pool/updates/main/h/html2ps/**	**LPRNG Runlpr & html2ps Command Execution**	**High**	**Bug discussed in newsgroups and websites.** ***Exploit script has been published.***
Trend Micro[103]	Multiple	InterScan VirusWall 3.6 Build 1182, l 3.6	A vulnerability exists when the CONNECT method is used because port usage on the proxy is not restricted, which could let a remote malicious user access arbitrary hosts on arbitrary ports.	Users should contact the vendor for details on obtaining upgrades.	InterScan VirusWall Unauthorized Proxy Connections	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Trend Micro, Inc.[104]	Windows 98/ME/2000 XP	OfficeScan Corporate Edition 5.02, PC-cillin 2003, 2002, 2000	A buffer overflow vulnerability exists in the mail scanning utility, which could let a malicious user cause a Denial of Service.	Upgrade available at: http://solutionfile.trendmicro.com/SolutionFile/12982/en	Trend Micro PC-cillin Mail Scanner Buffer Overflow	Low	Bug discussed in newsgroups and websites. Exploit script has been published.

[99] SuSE Security Announcement, SuSE-SA:2002:040, October 31, 2002.
[100] Debian Security Advisory, DSA 192-1, November 8, 2002.
[101] SecurityFocus, November 25, 2002.
[102] Debian Security Advisory, DSA 192-2, December 6, 2002.
[103] Bugtraq, December 5, 2002.
[104] Texonet Security Advisory 20021210, December 10, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Ultimate PHP Board[105]	Unix	Ultimate PHP Board 1.0 final beta	Several vulnerabilities exist: an information disclosure vulnerability exists in the 'add.php' script when an erroneous request is submitted, which could let a malicious user obtain sensitive information; a vulnerability exists in the 'viewtopic.php' script when a malicious request is submitted, which could let a malicious user obtain sensitive information; and a Cross-Site Scripting vulnerability exists in the 'viewtopic.php' script, which could let al malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	Ultimate PHP Board Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploits have been published for the 'viewtopic. php' script and Cross-Site Scripting vulnerabilities.
University of Cam-bridge[106]	Unix	Exim 3.35, 3.36, 4.10	A format string vulnerability exists in the daemon_go() function, which could let a malicious user execute arbitrary code with root privileges.	Patches available at: http://downloads.securityfocus.com/vulnerabilities/patches/	Exim Internet Mailer Format String	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
VBulletin [107]	Windows, Unix	VBulletin 2.2.7, 2.2.8	A vulnerability exists due to insufficient filtering of HTML code from posted messages, which could let a malicious user execute arbitrary HTML code.	No workaround or patch available at time of publishing.	vBulletin HTML Injection	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Webster [108]	Windows 95/98/ME/ NT 4.0/2000, XP	Webster HTTP Server	Multiple vulnerabilities exist: a buffer overflow vulnerability exists when malicious URLs are submitted, which could let a malicious user execute arbitrary code; a Directory Traversal vulnerability exists which could let a malicious user obtain sensitive information; and a Cross-Site Scripting vulnerability exists due to a failure to properly sanitize user-supplied input, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Webster HTTP Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Directory Traversal vulnerability can be exploited via a web browser. There is no exploit code required for the Cross-Site Scripting vulnerability.

[105] Bugtraq, December 7, 2002.
[106] Bugtraq, December 4, 2002.
[107] Bugtraq, December 8, 2002.
[108] Securiteam, December 2, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Xoops[109]	Windows, Unix	Xoops 1.3.5	A vulnerability exists in the Private Message System because HTML tags that are used for font attributes are not properly filtered, which could let a remote malicious user execute arbitrary HTML and script code.	Upgrade available at: http://www.xoops.org/modules/mydownloads/viewcat.php?cid=16 Patch available at: http://www.xoops.org/modules/mydownloads/singlefile.php?lid=265	Xoops Private Message System Font Attributes HTML Injection	High	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between November 29, and December 11, 2002, listed by date of script, script names, script description, and comments. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period, 21 scripts, programs, and net-news messages containing holes or exploits were identified. Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
December 11, 2002	Getad.c	Script that exploits the Windows 2000/XP WM_TIMER Message Handling vulnerability.
December 11, 2002	Getad2.c	Script that exploits the Windows 2000/XP WM_TIMER Message Handling vulnerability.
December 11, 2002	Raqrewt.c	Script that exploits the Cobalt RaQ4 Administrative Interface Command Execution vulnerability.
December 10, 2002	Pc-cillin.pl	Perl script that exploits the Trend Micro PC-cillin Mail Scanner Buffer Overflow vulnerability.
December 10, 2002	Sendfaild.c	Script that exploits the Sendmail local root vulnerability on BSD.

[109] SecurityTracker Alert ID, 1005770, December 6, 2002.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
December 8, 2002	Ethereal-0.9.8.tar.gz	A GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames.
December 8, 2002	**Prodos.sh**	**Script that exploits the ProFTPD STAT Command Denial of Service vulnerability.**
December 6, 2002	Libwhisker-1.6.tar.gz	A Perl module for performing whisker CGI vulnerability checks that adds a vast array of functionality and has robust functions that are geared toward network auditing.
December 6, 2002	Whisker-2.1.tar.gz	A high quality URL scanner which is used to search for known vulnerable CGIs on websites. Whisker does this by both scanning the CGIs directly as well as crawling the website in order to determine what CGIs are already currently in use.
December 4, 2002	Hoagie_exim.c	Script that exploits the Exim Internet Mailer Format String vulnerability.
December 4, 2002	Modjk-ex.	Exploit for the Apache/ Tomcat Mod_JK Chunked Encoding Denial of Service vulnerability.
December 4, 2002	S8exp.tar.gz	Solaris 8 local root exploit which uses ../../../tmp/module to cause priocntl(2) to load a module from anywhere.
December 4, 2002	**Zeroo-dir-traversal.pl**	**Perl script that exploits the Zeroo HTTP Server Directory Traversal vulnerability.**
December 4, 2002	**Zeroo-zemos.c**	**Perl script that exploits the Zeroo HTTP Server Directory Traversal vulnerability.**
December 3, 2002	Linksys_exploit.py	Exploit for the Multiple Linksys Vulnerabilities.
December 3, 2002	Snmp-traps.py	Exploit for the Multiple Linksys Vulnerabilities.
December 2, 2002	Epta.tgz	White paper on how to determine if a username is valid remotely by timing remote responses of login programs.
December 2, 2002	Lsrscan-0.5.tar.gz	Lsrscan scans remote hosts to determine if the will reverse source routed connections, and hence are vulnerable to spoofing attacks.
December 2, 2002	Nmap-3.10alpha4_statistics-1.diff	The Nmap 3.10ALFA Statistics Patch adds the -c switch which guesses how much longer the scan will take, shows how many ports have been tested, resent, and the ports per second rate.
December 2, 2002	Vncgame.c	VNC Game implements a man in the middle attack that bypasses VNC's challenge/response authentication, which keeps the password from being sniffed.
November 29, 2002	**Es-booz.c**	**Script that exploits the Boozt index.cgi Buffer Overflow vulnerability.**

Trends

- **The Internet security community has identified several new vulnerabilities in the Internet Software Consortium's (ISC) Berkeley Internet Name Domain (BIND) software, which is used by many ISPs to provide DNS services. The National Infrastructure Protection Center (NIPC) is issuing this advisory to heighten awareness to three newly identified vulnerabilities in BIND versions 4 and 8. For more information see NIPC Advisory 02-009, located at: http://www.nipc.gov/warnings/advisories/2002/02-009.htm and "Bugs, Holes & Patches" table.**
- **The CERT/CC has received reports that an intruder modified several of the released source code distributions of the libpcap and tcpdump packages and contain a Trojan horse. For more information see CERT® Advisory CA-2002-30, located at: http://www.cert.org/advisories/CA-2002-30.html and "Bugs, Holes & Patches" table.**
- **Multiple Kerberos distributions contain a remotely exploitable buffer overflow in the Kerberos administration daemon, which could let a remote malicious user obtain root privileges. The CERT/CC has received reports that indicate that this vulnerability is being**

exploited. For more information, see "Bugs, Holes & Patches" Table and CERT Advisory, CERT® Advisory CA-2002-29, located at: http://www.cert.org/advisories/CA-2002-29.html.

- **There have been a significant number of calls from customers concerned about a widespread e-mail that invites users to pick up an "E-Card" from a website called FriendGreetings.com. For more information, see http://www.sophos.com/virusinfo/articles/greetings.html.**
- **Firewalls and other systems that inspect FTP application layer traffic may not adequately maintain the state of FTP commands and responses. As a result, an attacker could establish arbitrary TCP connections to FTP servers or clients located behind a vulnerable firewall. For more information see Vulnerability Note VU#328867, located at: http://www.kb.cert.org/vuls/id/328867.**
- **The CERT/CC has received confirmation that some copies of the source code for the Sendmail package have been modified by an intruder to contain a Trojan horse. For more information, see "Bugs, Holes, & Patches Table" and CERT® Advisory CA-2002-28 located at: http://www.cert.org/advisories/CA-2002-28.html.**
- **The National Infrastructure Protection Center (NIPC) has issued an advisory to heighten the awareness of an e-mail-borne worm known as W32.Bugbear or I-Worm.Tanatos. For more information, see NIPC Advisory 02-008, located at: http://www.nipc.gov/warnings/advisories/2002/02-008.htm and Virus Section.**
- **The National Infrastructure Protection Center (NIPC) has been coordinating with the anti-virus and security community on the life cycle of "Slapper," the OpenSSL/Apache worm and all its variants. For more information, see NIPC ASSESSMENT 02-003, located at: http://www.nipc.gov/warnings/assessments/2002/02-003.htm.**
- **The SANS Institute and the National Infrastructure Protection Center (NIPC) have updated the list containing the Twenty Most Critical Internet Security Vulnerabilities. This list is broken into two categories: the ten most commonly exploited vulnerable services in Windows, and the ten most commonly exploited vulnerable services in Unix. For more detailed information, see: http://www.sans.org/top20.**

Viruses

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

BAT_BWG.J (Aliases: Bat/BWG.gen.b, I-Worm.BWG.d, Bat/ChinaBoy.Worm, VBS_BWG.J, IRC_BWG.J, REG_BWG.J) (Batch File Worm): This destructive batch file worm spreads through e-mail and Internet Relay Chat (IRC) using Microsoft Outlook and the chat client mIRC. It sends e-mail with the following details:

- Subject: Which pub in Singapore is the best in the world?
- Message Body: Read me to find out!!!
- Attachment: reame.TXT.bat

This batch file worm overwrites .REG, .VBS, .BAT, and .LNK files in the current directory, the parent directory, and the Windows directory and also drops copies of its components in all directories included in the environment variable PATH. This malware deletes known antivirus files and displays the following text:

- ChinaBlack rulez in Singapore!!!

JS/Newersaw (Internet Worm): This is an Internet worm that spreads through e-mail by using addresses it collects in the Microsoft Outlook Address Book. The worm arrives through e-mail and has various subjects and attachments. If executed, the worm copies itself in the following directories:

- C:\Windows\Start Menu\Programs\Startup\Startup.js
- C:\Windows\System\CMDWSH32.JS
- C:\Windows\System\FWD-MP3S.JS
- D:\Temporary.js

** Attempts to copy itself to all local drives as Temporary.js.

So that it gets run each time a user restart their computer the following registry keys get added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices "JSCmd32"="Wscript.exe C:\\WINDOWS\\SYSTEM\\CmdWsh32.js %1"

JS_VEREN.A (Aliases: JS.Nevezed, JS/Nevezed@MM, JS.Reven@mm, JS/Never.A@mm) (JavaScript Worm): This JavaScript malware behaves like a worm and executes on all Windows platforms. It uses Mail Application Program Interface applications to propagate via e-mail and network shared drives and sends e-mail messages to all e-mail addresses listed in the nearest active server of the network where the infected system is connected. In the network where the infected system is connected to, it searches for shared drives. It copies itself to a TEMPORARY.JS file in every shared drive it finds.

Kondrik@mm (Alias:I-Worm.Kondrik) (Internet Worm): Kondrik@mm sends itself to all addresses that it finds in the Microsoft Outlook Address Book. The e-mail will have the following characteristics:

- Subject: Wow! It should be seen"
- Attachment: Winpif.exe

When Kondrik@mm runs, it copies itself as C:\Windows\Winpif.exe and drops the file C:\Windows\Zp.vbs or C:\Windows\Sexxx.vbs. Next, the worm inserts one of these lines into the Autoexec.bat file:

- C:\Windows\zp.vbs
- C:\Windows\Sexxx.vbs

so that the worm runs when you start Windows (Windows 95/98/ME only).

VBS/Blaspheme (Visual Basic Script Worm): VBS/Blaspheme is an Internet worm that spreads through e-mail by using addresses it collects in the Microsoft Outlook Address Book. The worm arrives through e-mail and has various subject lines, message body and attachments. If executed, the worm copies itself in the \windows\%system% directory under the filenames "runmsdsk32.vbs" and "sitelist.vbs." So that it gets run each time a user restart their computer the following registry keys get added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\ Runmsdsk32=Runmsdsk32.vbs

The following file also gets created:

- HKEY_CURRENT_USER\Software\Theory\Theory\RecordContacts\

Then, it will search for files containing the following extensions: *.mp3, *.mp2, *.mpg, *.mpe, *.mpeg, *.avi, *.mov, and add the extension *.vbs to the file name.

VBS_HYPOTH.A (Aliases: VBS/LoveLetter.gen1, VBS/Pica.worm.gen, VBS.Hypoth@mm, VBS.Hypoth.A worm, I-Worm.Thery) (Visual Basic Script Worm): This Visual Basic Script (VBS) malware arrives and propagates copies of itself via e-mail. It sends different e-mail messages, each containing a copy of itself as attachment. This worm also appends an encrypted copy of itself in all VBS and VBE files listed on the infected system. It changes the extension names for files with the following extensions to VBS: mp3, mp2, mpg, mpe, mpeg, avi, and mov.

W32.HLLW.Datrix (Alias: Bloodhound.W32.5) (Win32 Worm): W32.HLLW.Datrix is a simple worm that copies itself to the shared folders of the KaZaA file-sharing network. The worm is written in the Microsoft Visual Basic programming language. When W32.HLLW.Datrix runs, it reads the registry value, "SharedDir," under the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Kazaa\CloudLoad

The worm then attempts to copy itself to the Windows\Kazaa\Cloudload folder, using the same file name as the file that was executed. The worm adds the value, "DarkMatrix <worm file name>," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the worm runs when you start Windows.

W32/HLLP.Hantaner (Aliases: W32.HLLP.Handy, @32/HLLP.Hantaner.A, Win32.HLLP.Hantaner) (Win32 Virus): This file-infecting virus specifically targets files that are downloaded from the web. When an infected file is run, it will infect only files with the suffix EXE that are in the download folders for either Internet Explorer or KaZaA and then will prepend the files it infects, regardless of whether they are truly executables, or just named as such. The specific location for the download directories will differ from one system to the next. For example, for KaZaA, this is generally \Program Files\KaZaA\My Shared Folder. The virus from the registry gleans the download folder information and if there are no download directories specified, the virus will not run. Files may be corrupted during infection such that they will no longer run, or they may run but they will not function correctly.

W32.Cervan.6256 (Win32 Virus): This is a virus that infects Windows Portable Executable (PE) files. The virus is polymorphic and entry-point obscuring (EPO).

W32.Heovin@mm (Win32 Worm): This is a mass-mailing worm that uses Microsoft Outlook to send itself to all contacts in Windows Address Book. It attempts to send a copy of itself to other mIRC users. It also has backdoor capabilities that allow a malicious user to remotely control an infected computer. The e-mail message has the following characteristics:

- The subject line is one of the following,
  - Subject: Flash funny pic or Subject: Check This update
- Message: Check dis out!
- Attachment: Funnyflush.pif

This threat is written in the Microsoft Visual Basic programming language.

W32.Hobble.H@mm (Alias: I-Worm.Alcaul.af) (Win32 Worm): This is a mass-mailing worm that replicates by e-mail and attempts to spread across the KaZaA file-sharing network. It also attempts to terminate the processes of various security related programs. W32.Hobble.H@mm is a .NET executable that is written in C# and runs only in the .NET Framework. The e-mail message has the following characteristics:

- Message Body: all we are saying, is give peace a chance. no to war and terrorism.
- Attachment: Topeace.exe

W32/Holar-C (Aliases: I-Worm.Galil, W32/Lagel.A, W32/SfxDeth.A-mm, W32.Galil@mm, W32.Holar.C@mm, W32/Holar.c@MM, Win32.Holar.C, WORM_HOLAR.C) (Win32 Worm): This appears to be a shockwave flash executable and displays a badly animated progress bar to mask its replication. After the progress bar reaches 100, the worm displays a message box containing the text "Looooooooool, thanx fo da time u spent thinkin ov me." Upon initial execution W32/Holar-C copies itself to iLLeGaL.exe in the Windows system folder and drops the hidden file Mplayer.exe in the same folder. The worm then sets the following registry entry to ensure its execution upon Windows startup:

- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\iLLeGaL

W32/Holar-C also sets increments the following registry entry every time it runs: HKLM\iLLeGaL The worm may activate a payload which deletes all files on drives D:, E:, F: and G:. W32/Holar-C looks for e-mail addresses in files on the hard drive and sends an e-mail to the addresses found.

W32.Lamin (Win32 Virus): W32.Lamin is a virus that infects Portable Executable (PE)* files. The virus also contains a keystroke logger and an IRC backdoor Trojan.

W32/Oror-K (Alias: W32.HLLW.Oror.B@mm) (W32 Worm): This is a worm which spreads by copying itself to shared folders on the local network and by e-mailing itself to addresses found within the inbox of MAPI based e-mail clients, such as Microsoft Outlook or Outlook Express. The e-mail subject, message text and attachment names are randomly chosen from a variety of possibilities. The worm attempts to exploit a MIME vulnerability in some versions of Microsoft Outlook, Microsoft Outlook Express, and Internet Explorer to allow the executable file to run automatically without the user double-clicking on the attachment. Microsoft has issued a patch that secures against this vulnerability that can be downloaded from http://www.microsoft.com/technet/security/bulletin/MS01-027.asp. (This patch fixes a number of vulnerabilities in Microsoft's software, including the one exploited by this worm.) When first run, the worm displays a message box with the text "Error starting program," "The <pathname of worm> file expects a newer version of Windows. Upgrade your Windows version.." The worm copies itself to the Windows folder with a name that is a combination of 'lib', the computer's name backwards and "16.exe," "32.exe" or "98.exe." For example if the computers name is "test," the worm copies itself as libtset16.exe, libtset32.exe or libtset98.exe. The worm creates the following registry entry so that the copy of the worm in the Windows folder is run automatically each time that Windows is restarted:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\LoadSystemProfile = <pathname of worm> powprof.dll,LoadCurrentUserProfile

The worm also sets the following registry entry to run itself automatically whenever an EXE file is executed:

- HKLM\Software\CLASSES\exefile\shell\open\command\(default) = <pathname of worm> "%1" %*.

W32/Oror-K chooses a random sub-folder of the Program Files folder and copies itself to this folder using the sub-folder name with "16.exe," "32.exe" or "2k.exe." For example, it might copy itself as \Program Files\Internet Explorer\Internet Explorer16.exe. The worm adds the pathname to this executable under the following registry key so that this copy of the worm is run automatically on startup:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run

The worm also copies itself to the Windows System folder using the name of a randomly selected file from the System folder, but with "16.exe," "32.exe" or "2k.exe" in place of the file's extension. The worm runs this copy of itself automatically on startup by adding the line run=<pathname of worm> to the [Windows] section of <Windows>\WIN.INI. W32/Oror-K spreads over the local network by copying itself to selected shared folders using random filenames. During this process the worm may create additional entries under the registry entry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run

The worm attempts to spread via file sharing on KaZaA networks by copying itself to any KaZaA folders it finds on the local network, using various filenames. W32/Oror-K also drops the mIRC script Controls.ini to the mIRC folder. The worm will attempt to terminate selected Windows based anti-virus programs.

W95/CIH.1106 (Word 97 Macro Virus): This W95/CIH variant was specifically rewritten to avoid detection. However, just like all other W95/CIH variants, it is detected in program heuristic mode as "New Win32" virus with any DATs. This variant has a dangerous payload that triggers when the CMOS clock is set to the 2nd date of a month. It would wipe flash BIOS on some computer models and overwrite data on the harddrive.

W97M_BEKO.A (Aliases: W97M/Beko.A@mm, WM97/Beko-A, Word97Macro/Beko.A:mm, W97M/Coke2k) (Word 97 Macro Virus): This macro virus infects Microsoft Word documents. To propagate, it drops a Visual Basic Script file to facilitate the sending of its copies via e-mail using Microsoft Outlook. It sends e-mail using this format to all addresses listed as contacts in the address book of the infected system:

- Subject: <filename of infected file without extension>
- Message Body: A confidential document is for you.. only for u!
- Attachment: <infected file>

If the system date is the 29th of any month, it displays these text strings:

- This Document is infected by Cokeboy Worm.

W97M.Omsee (Word 97 Macro Virus): W97M.Omsee is a macro virus that infects Microsoft Word documents and global template file, Normal.dot. W97M.Omsee activates when you open, close, or save a document, or exit Word. The virus creates the macro module "OmniSeek" and inserts itself into the document. It creates a file that contains the viral code as %windir%\OmniSeek.vbs. This file is detected as VBS.Omsee.

WM97/Forget-A (Alias: Macro.Word97.Forget) (Word 97 Macro Virus): On the 16th day of any month WM97/Forget-A will use the Office Assistant to display the message "- HOLA - NO SABEN QUIEN SOY ESTUPIDOS ...." This message will be repeated constantly. Once the virus is active, any attempt to access the Tools|Macro menu option will result in "Can not find application" being displayed.

WORM_ACEBOT.04 (Aliases: Win32/Acebot.B.Worm, Win32.Acebot.04 trojan, W32/AceBot.worm, W32.HLLW.Acebo, Worm.ACEBOT.A, Troj/Bdoor-ABN, Win32/Newbiero.0_4) (Internet Worm): This memory-resident malware exhibits characteristics of both a network worm and a backdoor program. As a worm, it propagates through drives connected to a local network. As a backdoor server program, it allows a remote user to perform any of the following on the infected system:

- launch a Distributed Denial Of Service (DDOS) attack via UDP (User Datagram
- Protocol) and IGMP (Internet Group Management Protocol)
- download and run files
- reboot, log off, shut down the machine
- update the server program
- kill the server program
- get system information (ISP, username, password, phone, Windows Path)
- get version number of certain applications
- share drive C
- log its activities and send a message via IRC

Aside from these backdoor capabilities, it also shuts down certain personal firewall applications and steals passwords from the infected system. It sends all the data it retrieves from the infected system to a remote malicious user via Internet Relay Chat (IRC), leaving the system adversely compromised.

WORM_AGOBOT.C (Aliases: Aliases: W32/Gaobot.worm.j, Backdoor.Agobot.040, Backdoor:Win32/Agobot.0_40, Win32.Agobot.040.A) (Internet Worm): This memory-resident worm propagates via the KaZaA, Grokster and Bearshare file-sharing networks and network shared drives. It regularly attempts to connect to an Internet Relay Chat (IRC) server as a bot. When connected, it may be used to launch Denial of Service (DoS) attacks against other users. This worm also has backdoor server capabilities and enables remote malicious users to access and manipulate infected systems. This worm works on Windows NT, 2000, and XP.

Worm/Escheri (Internet Worm): This is an Internet worm that copies itself into the Windows system directory under the filename "escherichia.exe." Once executed, it will remain in memory.

WORM_FORLORN.F (Aliases: Win32/Forlorn.f.Worm, W32/Forlorn-C, Win32/HLLW.Soltern.C, I-Worm.Soltern.c, W32/Sytro.worm.r) (Internet Worm): This worm uses its own Simple Mail Transfer Protocol (SMTP) engine to propagate via e-mail and retrieves addresses from the Windows Address Book (WAB) of the infected system. It is also designed to propagate via KaZaA and the Morpheus file-sharing networks. This worm waits for a three-minute interval before it sends out an e-mail to another target address.

WORM_GOP.F (Internet Worm): This worm propagates via e-mail and network shares. It sends the following e-mail with itself as attachment to all addresses listed in the infected user's Microsoft Outlook address book:

- Subject: <Chinese characters>
- Message Body: <Chinese characters>
- Attachment: photo.gif.exe

It drops a copy of itself as QQ2002.exe in network-shared drives and folders with read and write access. This worm steals the OICQ (Chinese version of ICQ) passwords of infected systems. It sends the stolen information to a specific e-mail address.

Worm/Kiltex (Internet Worm): This is a file sharing Internet worm that uses the file sharing networks KaZaA, eDonkey, Bearshare, and Swaptor to spread. If executed, the worm copies itself into the following directories:

- C:\windows\kilt.exe
- C:\kilt.exe
- C:\program files\windows media player\wmplayer.exe
- C:\windows\system32\screensaver.exe
- C:\program files\kazaa\my shared folder\kilt.exe
- C:\program files\kazaa\my shared folder\kilt game.exe
- C:\program files\edonkey2000\incoming\kilt game.exe
- C:\program files\edonkey2000\incoming\kilt.exe
- C:\program files\bearshare\shared\KILT GAME.exe
- C:\program files\Swaptor\Download\kilt.exe
- C:\program files\Swaptor\Download\KILT GAME.exe

Worm.P2P.Lolol (Alias: Lolol) (Internet Worm): This worm spreads via the KaZaA file sharing network. It has a powerful backdoor routine that connects to an IRC channel and listens to commands from its "master." The worm itself is a Windows PE EXE file about 60Kb of length written in Microsoft Visual C++. When infected file starts, the installation routine gets control.

Worm/Predig (Alias: W32/Prestige-A) (Internet Worm): This is an Internet worm that attempts to spread through e-mail by using addresses it collects from the Windows Address Book. It is social engineered to appear as photos of the sunken oil tanker Prestige that is currently leaking oil off the coast of Spain. The worm would arrive through e-mail in the following format:

- From: fotos_prestige@mareanegra.net
- Subject: fotos INEDITAS del PRESTIGE en el fondo del Atlantico!
- Body: <blank>
- Attachment: PRESTIG.zip

If executed, the worm copies itself in the \windows\%system% directory under the filename "PresTiGe.exe." Additionally, the files "m_prgrm.zip" (a zipped copy of itself), "m_Base64.xrf," and "m_WAB.XRF" (contains the retrieved e-mail addresses) get added in the \windows\%system% directory. It also renames the file regedit.exe (located in C:\windows) to m_regedit.exe. So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run XRF=C:\windows\%system%\PresTiGe.exe

Worm/ThreePigs (Internet Worm): Worm/ThreePigs arrives in a user inbox described as a story about the Three Little Pigs disguised under the screensaver Tarub.scr. The worm arrives through e-mail in the following format:

- Subject: Hello, I'm forwarding this for your kids.
- Attachment: Tarub.scr

If executed, the worm copies itself in the \windows\desktop directory under the filename "Tarub.scr." Worm/ThreePigs displays a very short story of the Three Little Pigs. If a user continues to click on to read they will eventually get to the end of the story and a message box so that they can send off the story to friends and family.

X97M.Sugar.F (Aliases: X97M/Sugar.gen, Macro.Excel97.Sugar.a) (Excel 97 Macro Virus): This is a variant of X97M.Sugar. This Microsoft Excel 97 macro virus adds the Visual Basic Application (VBA) module to an infected workbook. It adds its viral code to every worksheet in the workbook. The infection routine is triggered on activation or deactivation of an infected worksheet while editing in Excel. A worksheet is active when it is being edited. An active worksheet is deactivated when you edit another worksheet. This macro virus also creates a "BOOK1." file in the Excel startup folder, (usually \Office\XLSTART). By putting "BOOK1." in the Excel startup folder, the viral code is always loaded when you start Excel. The virus then creates the files C:\O6.reg and C:\O6.bat, and executes C:\O6.bat. It decrease the security levels of Excel by adding the value, "Options6 0x00000000," to the registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Office\8.0\Excel\Microsoft Excel

Yaha.J (Aliases: Lentin.H, I-Worm.Lentin.H, Yaha.H, W32/Lentin.G@mm) (Internet Worm): The Yaha.J worm was sent to over 50 different yahoogroups.com mailing lists on Friday the 13th of December 2002. This Yaha worm variant installs itself to system 3 times, creates a startup key for one of its files in the Registry and also modifies EXE file startup key so its other file could be started every time a user runs an EXE file. When run for the first time, Yaha.J displays a fake error message. Yaha.J spreads itself in e-mail messages with different subjects. It also spams numerous e-mail addresses by sending a message without its attachment there.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. Note: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	CyberNotes Issue #
AdClicker-J	**N/A**	**Current Issue**
AIM-Flood	N/A	CyberNotes-2002-16
Backdoor.AIMVision	N/A	CyberNotes-2002-21
Backdoor.Anakha	N/A	CyberNotes-2002-13
Backdoor.AntiLam	N/A	CyberNotes-2002-12
Backdoor.AntiLam.20	20	CyberNotes-2002-18
Backdoor.Antilam.g1	g1	CyberNotes-2002-23
Backdoor.Armageddon.B	N/A	CyberNotes-2002-20
Backdoor.Asniffer	N/A	CyberNotes-2002-21
Backdoor.Assasin	N/A	CyberNotes-2002-14
Backdoor.Assasin.B	B	CyberNotes-2002-23
Backdoor.Assasin.C	C	CyberNotes-2002-24
Backdoor.Baste	N/A	CyberNotes-2002-23
Backdoor.Bofishy.C	C	CyberNotes-2002-23
Backdoor.Cabro	N/A	CyberNotes-2002-17
Backdoor.Cabrotor	N/A	CyberNotes-2002-18
Backdoor.Cigivip	N/A	CyberNotes-2002-23
Backdoor.Coreflood	**N/A**	**Current Issue**
Backdoor.Crat	N/A	CyberNotes-2002-12
Backdoor.Cyn	N/A	CyberNotes-2002-18
Backdoor.DarkFtp	N/A	CyberNotes-2002-19

Trojan	Version	CyberNotes Issue #
Backdoor.DarkSky.B	B	CyberNotes-2002-20
Backdoor.DarkSky.C	C	CyberNotes-2002-21
Backdoor.Delf	N/A	CyberNotes-2002-16
Backdoor.Delf.B	B	CyberNotes-2002-16
Backdoor.Delf.C	C	CyberNotes-2002-17
Backdoor.Delf.D	D	CyberNotes-2002-22
Backdoor.Delf.E	E	CyberNotes-2002-24
Backdoor.Denwp	**N/A**	**Current Issue**
Backdoor.Dindang	N/A	CyberNotes-2002-22
Backdoor.Ducktoy	N/A	CyberNotes-2002-15
Backdoor.Easyserv	N/A	CyberNotes-2002-16
Backdoor.Elitem	N/A	CyberNotes-2002-20
Backdoor.Evilbot	N/A	CyberNotes-2002-09
Backdoor.Expjan	N/A	CyberNotes-2002-18
Backdoor.Feardoor	N/A	CyberNotes-2002-21
Backdoor.Fearic	N/A	CyberNotes-2002-16
Backdoor.FTP_Ana	N/A	CyberNotes-2002-20
Backdoor.FTP_Ana.B	B	CyberNotes-2002-20
Backdoor.FTP_Bmail	N/A	CyberNotes-2002-12
Backdoor.Fulamer.25	N/A	CyberNotes-2002-24
Backdoor.FunFactory	N/A	CyberNotes-2002-19
Backdoor.GF.13	N/A	CyberNotes-2002-23
Backdoor.Ghoice.12	**N/A**	**Current Issue**
Backdoor.Goster	N/A	CyberNotes-2002-20
Backdoor.GRM	N/A	CyberNotes-2002-13
Backdoor.GSpot	N/A	CyberNotes-2002-12
Backdoor.GWGhost	N/A	CyberNotes-2002-21
Backdoor.Hatckel	**N/A**	**Current Issue**
Backdoor.Helios	N/A	CyberNotes-2002-19
Backdoor.Hupigeon	N/A	CyberNotes-2002-21
Backdoor.IrcContact	N/A	CyberNotes-2002-24
Backdoor.Kaitex.B	B	CyberNotes-2002-20
Backdoor.Kaitex.C	C	CyberNotes-2002-22
Backdoor.Kavar	N/A	CyberNotes-2002-16
Backdoor.Klb	N/A	CyberNotes-2002-22
Backdoor.Kryost	N/A	CyberNotes-2002-18
Backdoor.Lanfilt	N/A	CyberNotes-2002-24
Backdoor.Lanfiltrator	**N/A**	**Current Issue**
Backdoor.Laphex	N/A	CyberNotes-2002-18
Backdoor.Laphex.Client	N/A	CyberNotes-2002-18
Backdoor.Lastdoor	N/A	CyberNotes-2002-18
Backdoor.Latinus	N/A	CyberNotes-2002-12
Backdoor.Latinus.B	B	CyberNotes-2002-18
Backdoor.Litmus.203.b	B	CyberNotes-2002-22
Backdoor.Litmus.2a	2a	CyberNotes-2002-20
Backdoor.LittleWitch.B	B	CyberNotes-2002-22
Backdoor.Lolok	**N/A**	**Current Issue**
Backdoor.Malpayo	N/A	CyberNotes-2002-24

Trojan	Version	CyberNotes Issue #
Backdoor.Mapsy	**N/A**	**Current Issue**
Backdoor.Miffice	N/A	CyberNotes-2002-18
Backdoor.Mirab	N/A	CyberNotes-2002-13
Backdoor.Miranda	**N/A**	**Current Issue**
Backdoor.Mite	N/A	CyberNotes-2002-18
Backdoor.MLink	N/A	CyberNotes-2002-16
Backdoor.Ndad	N/A	CyberNotes-2002-17
Backdoor.Neodurk	N/A	CyberNotes-2002-23
Backdoor.NetControle	N/A	CyberNotes-2002-13
Backdoor.Niovadoor	N/A	CyberNotes-2002-22
Backdoor.Nota	N/A	CyberNotes-2002-12
Backdoor.Omed.B	B	CyberNotes-2002-11
Backdoor.Optix.04	04	CyberNotes-2002-19
Backdoor.Optix.04.b	B	CyberNotes-2002-22
Backdoor.Optix.04.c	C	CyberNotes-2002-22
Backdoor.OptixPro.10	10	CyberNotes-2002-18
Backdoor.OptixPro.11	11	CyberNotes-2002-20
Backdoor.OptixPro.11.b	B	CyberNotes-2002-22
Backdoor.OptixPro.12	12	CyberNotes-2002-18
Backdoor.Osirdoor	N/A	CyberNotes-2002-17
Backdoor.Pest.Cli	N/A	CyberNotes-2002-20
Backdoor.Pestdoor	N/A	CyberNotes-2002-20
Backdoor.Phoenix	N/A	CyberNotes-2002-19
Backdoor.Platrash	N/A	CyberNotes-2002-21
Backdoor.Ptakks.B	N/A	CyberNotes-2002-18
Backdoor.RCServ	N/A	CyberNotes-2002-19
Backdoor.RemoteNC	N/A	CyberNotes-2002-09
Backdoor.RemoteNC.B	B	CyberNotes-2002-24
Backdoor.Revrs	N/A	CyberNotes-2002-22
Backdoor.Ripjac	N/A	CyberNotes-2002-24
Backdoor.RMFDoor.Cli	N/A	CyberNotes-2002-20
Backdoor.Robi	N/A	CyberNotes-2002-18
Backdoor.Roxrat.10	N/A	CyberNotes-2002-20
Backdoor.Roxrat.12	**N/A**	**Current Issue**
Backdoor.Sazo	N/A	CyberNotes-2002-13
Backdoor.Scanboot	N/A	CyberNotes-2002-17
Backdoor.Sdbot.B	B	CyberNotes-2002-22
Backdoor.Seamy	N/A	CyberNotes-2002-18
Backdoor.Singu	N/A	CyberNotes-2002-22
Backdoor.Skun	**N/A**	**Current Issue**
Backdoor.Sparta	N/A	CyberNotes-2002-13
Backdoor.Sparta.B	B	CyberNotes-2002-19
Backdoor.Sparta.C	C	CyberNotes-2002-21
Backdoor.Spigot.B	B	CyberNotes-2002-22
Backdoor.Spoofbot	N/A	CyberNotes-2002-24
Backdoor.StealthEye	**N/A**	**Current Issue**
Backdoor.Synrg	N/A	CyberNotes-2002-22
Backdoor.Tela	N/A	CyberNotes-2002-17

Trojan	Version	CyberNotes Issue #
Backdoor.Theef	N/A	CyberNotes-2002-15
Backdoor.Theef.B	B	CyberNotes-2002-21
Backdoor.Theef.C	**C**	**Current Issue**
Backdoor.Tourniq	**N/A**	**Current Issue**
Backdoor.Tron	N/A	CyberNotes-2002-12
Backdoor.Ultor	N/A	CyberNotes-2002-13
Backdoor.VB.CH	**N/A**	**Current Issue**
Backdoor.WinShell	N/A	CyberNotes-2002-16
Backdoor.Wiween	N/A	CyberNotes-2002-22
Backdoor.Wold	N/A	CyberNotes-2002-22
Backdoor.Y3KRat.14	N/A	CyberNotes-2002-24
Backdoor.Y3KRat.15	N/A	CyberNotes-2002-17
Backdoor.Zenmaster	N/A	CyberNotes-2002-19
Backdoor-AKO	N/A	CyberNotes-2002-20
BackDoor-AKR	N/A	CyberNotes-2002-19
BackDoor-AKW	**N/A**	**Current Issue**
BackDoor-ALT	N/A	CyberNotes-2002-21
BackDoor-AMB	N/A	CyberNotes-2002-22
BackDoor-AMH	N/A	CyberNotes-2002-23
Banan.Trojan	N/A	CyberNotes-2002-15
Bck/Litmus.201	N/A	CyberNotes-2002-14
BDS/ConLoader	N/A	CyberNotes-2002-12
BDS/EHKSLogger	N/A	CyberNotes-2002-19
BDS/Pestdoor.4	N/A	CyberNotes-2002-20
BDS/SDbot.XY	**N/A**	**Current Issue**
BDS/Sporkbot	N/A	CyberNotes-2002-20
BDS/WinSpyer	N/A	CyberNotes-2002-22
BKDR_EMULBOX.A	N/A	CyberNotes-2002-10
BKDR_INTRUZZO.A	N/A	CyberNotes-2002-09
BKDR_LITMUS.C	N/A	CyberNotes-2002-09
Bneo.Trojan	N/A	CyberNotes-2002-18
Cardst	N/A	CyberNotes-2002-17
Cytron	N/A	CyberNotes-2002-20
Diskfill-F	F	CyberNotes-2002-23
Downloader.BO.dr	dr	CyberNotes-2002-24
Downloader-BO.b	b	CyberNotes-2002-23
FakeGina.Trojan	N/A	CyberNotes-2002-16
Fortnight	N/A	CyberNotes-2002-10
IIS.Beavuh-Exploit	N/A	CyberNotes-2002-17
IRC.kierz	N/A	CyberNotes-2002-16
Jekord	N/A	CyberNotes-2002-19
JS/NoClose	N/A	CyberNotes-2002-11
Liquid.Trojan	N/A	CyberNotes-2002-14
Netbus.160.Dropper	N/A	CyberNotes-2002-17
Poldo	**N/A**	**Current Issue**
PWS-AOLFake	N/A	CyberNotes-2002-15
PWS-MSNCrack	N/A	CyberNotes-2002-18
PWS-MSNSteal	N/A	CyberNotes-2002-17
PWS-Ritter	N/A	CyberNotes-2002-16

Trojan	Version	CyberNotes Issue #
PWSteal.Antigen	N/A	CyberNotes-2002-23
PWSteal.Avisa	N/A	CyberNotes-2002-24
PWSteal.BStroj	N/A	CyberNotes-2002-20
PWSteal.Fender	**N/A**	**Current Issue**
PWSteal.Kaylo	N/A	CyberNotes-2002-17
PWSteal.Netsnake	N/A	CyberNotes-2002-17
PWSteal.Profman	N/A	CyberNotes-2002-17
PWSteal.SoapSpy	N/A	CyberNotes-2002-18
QDel227	N/A	CyberNotes-2002-09
QDel234	N/A	CyberNotes-2002-11
QDel297	N/A	CyberNotes-2002-23
QDel350	N/A	CyberNotes-2002-24
QDel356	**N/A**	**Current Issue**
RCServ	N/A	CyberNotes-2002-10
Reboot-R	N/A	CyberNotes-2002-18
Reboot-T	**N/A**	**Current Issue**
StartPage-B	N/A	CyberNotes-2002-16
Swporta.Trojan	N/A	CyberNotes-2002-13
TR/EvilDX	N/A	CyberNotes-2002-19
Tr/FakeYahoMe	N/A	CyberNotes-2002-23
Tr/Mastaz	N/A	CyberNotes-2002-23
Tr/SCKeyLog.Spy.20	N/A	CyberNotes-2002-22
TR/Win32.Rewin	N/A	CyberNotes-2002-12
Tr/WiNet	N/A	CyberNotes-2002-10
TR/WLoader	N/A	CyberNotes-2002-20
TR/Zirko	N/A	CyberNotes-2002-10
Trj/GhostGirl	N/A	CyberNotes-2002-19
Troj/Apher-A	N/A	CyberNotes-2002-17
Troj/Bdoor-AML	N/A	CyberNotes-2002-23
Troj/Diablo	N/A	CyberNotes-2002-09
Troj/DSS-A	N/A	CyberNotes-2002-12
Troj/FireAnv-A	N/A	CyberNotes-2002-19
Troj/Flood-O	N/A	CyberNotes-2002-14
Troj/Kbman	N/A	CyberNotes-2002-10
Troj/Momma-B	N/A	CyberNotes-2002-11
Troj/Netdex-A	N/A	CyberNotes-2002-21
Troj/Nethief-C	N/A	CyberNotes-2002-22
Troj/Ritter-A	N/A	CyberNotes-2002-17
Troj/Tobizan-A	N/A	CyberNotes-2002-16
Troj/Tubmo-A	**N/A**	**Current Issue**
Troj/Unreal-A	N/A	CyberNotes-2002-16
Troj/Zasil-A	N/A	CyberNotes-2002-23
TROJ_DOAL.A	N/A	CyberNotes-2002-14
TROJ_FLOOD.BI.DR	**N/A**	**Current Issue**
TROJ_INOR.A	A	CyberNotes-2002-23
TROJ_INOR.B	B	CyberNotes-2002-23
TROJ_JUNTADOR.G	N/A	CyberNotes-2002-10
TROJ_OPENME.B	N/A	CyberNotes-2002-09
TROJ_SMALL.J	N/A	CyberNotes-2002-10

Trojan	Version	CyberNotes Issue #
TROJ_SMBNUKE.A	N/A	CyberNotes-2002-18
TROJ_SQLSPIDA.B	N/A	CyberNotes-2002-11
TROJ_SUOMIA.A	N/A	CyberNotes-2002-18
TROJ_WORTRON.10B	N/A	CyberNotes-2002-12
Trojan.Adclicker	N/A	CyberNotes-2002-19
Trojan.Adnap	N/A	CyberNotes-2002-17
Trojan.Ahero	N/A	CyberNotes-2002-24
Trojan.Allclicks.A	N/A	CyberNotes-2002-13
Trojan.AntiUpdater	N/A	CyberNotes-2002-23
Trojan.Avid	N/A	CyberNotes-2002-19
Trojan.Beway	N/A	CyberNotes-2002-15
Trojan.Crabox	N/A	CyberNotes-2002-17
Trojan.DiabKey	N/A	CyberNotes-2002-18
Trojan.Diskfil	N/A	CyberNotes-2002-19
Trojan.Downloader.Cile	**N/A**	**Current Issue**
Trojan.Fatkill	N/A	CyberNotes-2002-09
Trojan.Houpe	N/A	CyberNotes-2002-23
Trojan.Iblis	N/A	CyberNotes-2002-22
Trojan.IrcBounce	N/A	CyberNotes-2002-19
Trojan.Junnan	N/A	CyberNotes-2002-16
Trojan.Lovead	N/A	CyberNotes-2002-19
Trojan.Nullbot	N/A	CyberNotes-2002-19
Trojan.Portacopo:br	N/A	CyberNotes-2002-16
Trojan.Prova	N/A	CyberNotes-2002-10
Trojan.PSW.Ajim_bbs	N/A	CyberNotes-2002-19
Trojan.PSW.CrazyBilets	N/A	CyberNotes-2002-12
Trojan.PSW.M2	N/A	CyberNotes-2002-13
Trojan.PWS.QQPass.C	N/A	CyberNotes-2002-21
Trojan.Starfi	N/A	CyberNotes-2002-16
Trojan.Win32.Filecoder	N/A	CyberNotes-2002-18
Trojan.Win32.MSNTrick	N/A	CyberNotes-2002-17
Trojan.WinReboot	N/A	CyberNotes-2002-20
UNIX_ALUTAPS.A	N/A	CyberNotes-2002-21
VBS.AVFake	N/A	CyberNotes-2002-22
VBS.Krim.C	N/A	CyberNotes-2002-22
VBS.Lavra.B.Worm	N/A	CyberNotes-2002-19
VBS.Zevach	N/A	CyberNotes-2002-15
VBS/Helvis	N/A	CyberNotes-2002-22
W32.Azak	N/A	CyberNotes-2002-16
W32.Balick.Trojan	N/A	CyberNotes-2002-24
W32.Cbomb	N/A	CyberNotes-2002-16
W32.Click	N/A	CyberNotes-2002-15
W32.Darkgoose.Trojan	N/A	CyberNotes-2002-24
W32.DSS.Trojan	N/A	CyberNotes-2002-09
W32.Estrella	N/A	CyberNotes-2002-13
W32.Evala.Worm	N/A	CyberNotes-2002-14
W32.IRCBot	N/A	CyberNotes-2002-14
W32.Kamil	N/A	CyberNotes-2002-16
W32.Kotef	N/A	CyberNotes-2002-16

Trojan	Version	CyberNotes Issue #
W32.Libi	N/A	CyberNotes-2002-10
W32.Manifest.Trojan	N/A	CyberNotes-2002-24
W32.Nuker.Winskill	N/A	CyberNotes-2002-15
W32.STD.D	N/A	CyberNotes-2002-22
W32.Tendoolf	N/A	CyberNotes-2002-09
W32.Wabbin	N/A	CyberNotes-2002-15
WbeCheck	N/A	CyberNotes-2002-09
Winshell	N/A	CyberNotes-2002-15
Worm/Garra	N/A	CyberNotes-2002-20
X97M.Feng.A.Trojan	**N/A**	**Current Issue**

AdClicker-J (Alias: TROJ_TIBBAR.A): When running this Trojan repeatedly attempts to connect to a remote web site. When executed on the victim machine, a fake message box is displayed and a minimized window title bar can be seen. The Trojan copies itself into the Windows directory as SNDVOL.EXE. Subsequently, it hooks system startup by adding the following Registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "Cron" = "C:\WINDOWS\sndvol.exe"

This Registry hook is removed when cleaning with the indicated engine/DATs. Additionally, the following Registry key is created, indicating the Trojan's (installed) presence:

- HKEY_CURRENT_USER\Software\Rabbit "Exec" = "1"

BackDoor-AKW (Alias: Backdoor.Remoper): This is a remote access Trojan. It is comprised of two components. A server component which once running on the victim machine, enables the malicious user to connect (and administer that machine) using the client component. The server component may be installed via a dropper. At least one such dropper received by AVERT has been misleadingly named 'NortonAntiVirus.exe'. When run, the dropper installs the server component in the Windows System directory as WIN32RT.EXE. System startup is hooked via the addition of the following key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "Wi32De75" = C:\WINDOWS\SYSTEM\WIN32RT.EXE

The server component also opens port 6066 on the victim machine. The client component enables the malicious user to connect to remote victim machines with the server installed.

Backdoor.Coreflood: This is a backdoor Trojan that is designed primarily to conduct Denial of Service attacks. The Trojan connects to an IRC server and gives control of the infected computer to a malicious user. The Trojan consists of two parts:

- An .exe file, which is the loader
- A .dll file, which contains the primary code.

When the Trojan runs, it extracts the .dll file from itself and copies itself and the .dll file to the %system% folder. The file names are arbitrary. The .exe file then calls a function within the .dll file to begin execution of the main code. The main code hooks the Explorer.exe process in a way that all of its actions run under the process context of Explorer.exe. When the main code is run, the Trojan adds the value, "<file name> %system%\<file name.ext>," to the registry key:

- HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/Run

so that the Trojan runs each time that you start Windows. The Trojan monitors this registry key and may add it again if it is modified or removed. The Trojan then connects to an IRC server and joins a predefined chat channel. It listens for commands to execute. These commands allow a malicious user to gain unauthorized access to an infected computer.

Backdoor.Denwp: Backdoor.Denwp allows a malicious user to remotely control an infected computer. It is written in the Microsoft Visual Basic programming language. When Backdoor.Denwp runs, it copies itself as C:\%windir%\Systimeupdate.exe and adds the value, "System-Time Update C:\%windir%\systimeupdate.exe," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you restart Windows. The Trojan then opens an HTTP connection to a Web server that the malicious user chooses and posts information that it steals from you to a script at that Web site. It also opens many TCP and UDP ports and allows the malicious user to launch a DDoS (Distributed Denial of Service) attack from the compromised computer.

Backdoor.Ghoice.12: Backdoor.Ghoice.12 allows unauthorized access to the infected computer. It is written in the Microsoft Visual Basic programming language. When Backdoor.Ghoice.12 runs, it copies itself to the %windir% folder using a file name that is chosen by the malicious user. It then adds a value that refers to the dropped Trojan file to the registry key:

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

The name of the value may vary; by default, it copies itself as C:\%windir%\Shell12.exe, and adds the value,"command C:\%Windir%\shell12.exe." It may also create C:\%system%\Xvoice.dll, which is 89,800 bytes in size. The Trojan opens a TCP port for the malicious user to connect to the computer. The TCP port that it uses may vary. The default port number is 1001. The Trojan waits for commands from the malicious user. If your computer has speakers connected to it, you may hear various phrases that have been chosen by the a malicious user.

Backdoor.Hatckel (Aliases: Backdoor.VB.ck, Generic BackDoor): This is a backdoor Trojan that gives an attacker unauthorized access to an infected computer. By default it opens 15 ports on the infected computer: 1101 to 1115. Backdoor.Hatckel is written in Visual Basic. When Backdoor.Hatckel runs, it creates the value, "Runths <Trojan path and file name>," in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan starts when you start Windows. It creates or modifies the values:

- Search Page http:/www.telhack.org
- Söksida http:/www.telhack.org
- Startsida http:/www.telhack.org

in the registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main

If the operating system is Windows 95/98/ME, Backdoor.Hatckel attempts to obtain access to the password cache that is stored on the local computer. To notify the client side, the Trojan uses ICQ pager notification.

Backdoor.Lanfiltrator (Alias: Backdoor.LanFiltrator.10): This is a backdoor Trojan that gives an attacker unauthorized access to a compromised computer. The detection is used for a family of Trojans that are produced by the Backdoor.Lanfiltrator generator.

Backdoor.Lolok: This is a backdoor Trojan that uses the mIRC client to give a malicious user access to the computer. It typically arrives in an e-mail message or is presented for download over an IRC channel. It may be disguised as a video file. When Backdoor.Lolok runs, it creates the file, "%windir%\Temp\Irsetup.exe," and the subfolder, "%windir%\System\Helpus," where it places the remainder of the files that it creates. Backdoor.Lolok creates the value, "System %windir%\SYSTEM\HELPUS\INTIRNAT.EXE," in the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs each time that you start Windows. Backdoor.Lolok also modifies the run= line of the Win.ini file to run=C:\. By default, Backdoor.Lolok establishes an IRC connection to irc.tu-pac.net on port 9876. It then sends a notification message to the malicious user. This allows the malicious user to send commands to the backdoor, which then carries out the commands. For example, it can upload and download files, execute scripts, and so on.

Backdoor.Mapsy (Aliases: Backdoor.IRC.Mapsy, BackDoor-AMI, BKDR_IRCMAPSY.A): This is a backdoor Trojan that gives an attacker unauthorized access to an infected computer. By default it opens and listens on port 6754. Backdoor.Mapsy is packed with UPX v1.21. When Backdoor.Mapsy runs, it copies itself as SysMap.exe into the %system% folder and drops a file named SysMap.dll (31,232 bytes) into the %system% folder. The Trojan creates the value,v" Microsoft® System Mapper %system%\SysMap.exe," in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan starts when you start Windows. If the operating system is Windows 95/98/ME, then the Trojan registers itself as a service process to continue to run after the user logs off. Also, the Trojan installs hook procedures into a hook chain to monitor the system for keyboard and mouse messages. This permits Backdoor.Mapsy to intercept keystrokes. The Trojan uses ICQ pager to notify the client side. After Backdoor.Mapsy is installed, it awaits commands from the remote client through IRC channels.

Backdoor.Miranda: Backdoor.Miranda allows a malicious user to remotely control an infected computer. The Trojan uses an ICQ paging function to send the victim's system information to the malicious user. It is written in the Borland Delphi programming language and is compressed with UPX. When Backdoor.Miranda runs, it copies itself into the C:\%system% folder. The exact file names that are used by the Trojan may vary from version to version because the malicious user who creates this backdoor Trojan can choose any desired file name. By default, the file name is System32.exe. The Trojan adds a value, which refers to the dropped Trojan file, to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows. The Trojan then opens an HTTP connection to make use of an ICQ paging function to send the victim's information to the malicious user. It opens many TCP ports. After Backdoor.Miranda is installed, it waits for commands from the remote client.

Backdoor.Roxrat.12: This is a variant of Backdoor.Roxrat. It gives an attacker unauthorized access to an infected computer. The Trojan attempts to disable some major antivirus and firewall products by terminating the active processes that are in a list that the Trojan maintains. It opens TCP ports 10666, 65000, and 65010 to connect to the malicious user. This threat is written in the Borland Delphi programming language.

Backdoor.Skun (Alias: Backdoor.Skun.001): This is a Backdoor Trojan that gives an attacker unauthorized access to an infected computer. It attempts to log keystrokes to capture confidential information. Backdoor.Skun is packed with UPX v1.20. When Backdoor.Skun runs, it copies itself as %system%\Task.tsk. The Trojan creates the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.tsk

and adds the following values to this key:

- (Default) exefile
- Content Type application/x-msdownload

Then, the Trojan creates the value, "Microsoft Task Control %system%\task.tsk," in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan starts when you start Windows. In addition, the Trojan adds the value, "run %system%\task.tsk," to the registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

If the operating system is Windows 95/98/ME, the Trojan registers itself as a service process so that it continues to run after you log off. Backdoor.Skun attempts to obtain access to the password cache that is stored on the local computer. It installs hook procedures into a hook chain to monitor the system for keyboard and mouse messages. This permits Backdoor.Skun to intercept keystrokes. After Backdoor.Skun is installed, it waits for commands from the remote client.

Backdoor.StealthEye (Alias: Backdoor.StealthEye.11): This is a backdoor Trojan that gives an attacker unauthorized access to an infected computer. By default it opens ports 9777 and 9778 on the infected computer. Backdoor.StealthEye is written in Visual Basic. When Backdoor.StealthEye runs, it copies itself as C:\Windows\System\Camdrv.exe and creates the value, "cam C:\Windows\System\Camdrv.exe," in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan starts when you start Windows. After Backdoor.StealthEye is installed, it waits for commands from the remote client.

Backdoor.Theef.C (Aliases: Backdoor Backdoor.Theefle.111, Backdoor-AFG, BKDR_AFG.A): This is a backdoor Trojan that gives an attacker unauthorized access to an infected computer. By default it opens and listens on port 13298. When Backdoor.Theef.C is executed, it copies itself as, "windir%\WinVid32.exe," and creates the value, "WinVidix %windir%/WinVid32.exe," in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan starts when you start Windows. If the operating system is Windows 95/98/ME, the Trojan registers itself as a service process so that it continues to run after you log off. The Trojan uses ICQ pager to notify the client side. After Backdoor.Theef.C is installed, it waits for commands from the remote client.

Backdoor.Tourniq (Alias: Backdoor.Tourniq.11): Backdoor.Tourniq allows a malicious user to remotely control an infected computer. It is written in the Microsoft Visual Basic programming language. When Backdoor.Tourniq runs, it copies itself as C:\%system%\iexplorer.exe and adds the value, "winsys C:\%system%\iexplorer.exe," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows. It opens a TCP port 6666 to connect to the malicious user. After Backdoor.Tourniq is installed, it waits for commands from the remote client.

Backdoor.VB.CH: This is a backdoor Trojan that opens a port on the computer. It also sends an e-mail message that contains the IP address of the infected computer to the Trojan's author. When Backdoor.VB.CH runs, it first, it adds the value, "systray <path and file name>," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

so that it runs each time that you start Windows. Next, the Trojan sends an e-mail message to the author of the Trojan. The message contains the IP address of the infected computer, as well as its registered Windows name. Finally, Backdoor.VB.CH opens a port on the computer to allow incoming connections.

BDS/SDbot.XY: Like other backdoors, BDS/SDbot.XY would potentially allow someone with malicious intent remote access to your computer. If executed, the backdoor adds the following file to the \windows\ directory, "Lmass.exe." So that it gets run each time a user restart their computer the following registry keys get added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "Configuration Loader"="lmass.exe"
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices "Configuration Loader"="lmass.exe"

PWSteal.Fender: PWSteal.Fender claims to be a tool to automate actions in the Diablo II game. However, the program actually e-mails Diablo II account details to a Hotmail address. When PWSteal.Fender runs, it displays a configuration window that prompts you for account settings. After you click Start, the account details are mailed to a Hotmail address through Microsoft Outlook. PWSteal.Fender then attempts to launch the executable located at C:\Program Files\Diablo II\Diablo II.exe. If Diablo II has been installed to a custom folder or is not installed, you will see an error message.

Poldo: This trojan poses as an anti-virus program and a file commonly associated with an e-mail hoax. The trojan is designed to display popup windows and alter the default search page, and start page of Internet Explorer.

QDel356: This file purports to be a virus removal application. Upon running, this trojan displays the an error message. The trojan searches the Windows directory for specific files which it will delete, if found:

- taskbar.bak
- taskbar.exe
- notepad.ini
- win64.ini
- winstat.ini
- wbackup.ini
- wcurrent.ini
- winhelp.ini

As the file is not referenced in startup locations and it does not stay in memory, once the file is run initially, it will not perform any further actions without being run again manually.

Reboot-T: This trojan sets a Registry key such that the victim machine restarts upon booting Windows. In testing, it does not work as designed on NT systems. When run on the victim machine, the following dialog box is displayed ('Installation Successful' in German). The following Registry key is also set:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "Sdll32" = rundll32.exe user,exitWindows

Troj/Tubmo-A: This Trojan has been reported in the wild. It is an executable program that attempts to download a file from a remote website. When the Trojan is first run it asks the user to enter a password. If the password is accepted the file is downloaded from the remote website. The executable file downloaded could be a backdoor Trojan that would compromise the security of the user's computer.

TROJ_FLOOD.BI.DR: This Trojan is a backdoor package that drops and installs a multi-component backdoor in the System directory. The dropped multi-component backdoor, which is detected as several malware, allows malicious users to remotely take control of infected systems. This backdoor package can force infected systems into behaving as FTP servers, allowing remote users to upload and download files to and from infected machines. It also contains IRC scripts that may be used to launch a Distributed Denial of Service (DDoS) attack. With the scripts installed, malicious users can manipulate infected systems into flooding certain targets within IRC by continuously PING-ing these targets. This Trojan arrives as an installation/setup program, and runs on Windows 9x, ME, 2000, and XP.

Trojan.Downloader.Cile: This is a Trojan horse that attempts to download files from a specified Web site and execute them. When Trojan.Downloader.Cile is executed, it first attempts to copy the following files to the %windir% folder:

- Registry.dll
- Registry.exe
- Rt.dll

Next, the Trojan adds the value, “Registry Services %windir%\Registry.exe,” to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs each time that you start Windows. Finally, the Trojan attempts to download some files from a specific Web site. If this is successful, the Trojan executes them. Currently, these files contain Backdoor.Delf,

X97M.Feng.A.Trojan: This is a Trojan horse that resides in Microsoft Excel documents. When X97M.Feng.A.Trojan runs, it deletes:

- All files that are located in the same folder as the infected workbook
- All files that are located in the C:\My Documents folder
- C:\io.sys
- C:\Config.sys
- C:\Msdos.sys
- C:\Command.com

X97M.Feng.A.Trojan then saves itself as %Excel Startup%\Fuck.xls. This allows X97M.Feng.A.Trojan to be executed each time that another workbook is opened, during which time it deletes all sheets from the workbook. Finally X97M.Feng.A.Trojan saves itself as:

- C:\io.sys
- C:\Msdos.sys

It then restarts the computer. As a result of the file deletions and replacements, if the operating system is Windows 95/98/ME, the computer will no longer start.